# Computational Arithmetic Geometry I: Sentences Nearly in the Polynomial Hierarchy[1]

J. Maurice Rojas[2]

E-mail: mamrojas@math.cityu.edu.hk

*Department of Mathematics, Texas A&M University, College Station, Texas 77843-3368, USA (after January 2001).*[3]

DEDICATED TO GRETCHEN DAVIS.

We consider the average-case complexity of some otherwise undecidable or open Diophantine problems. More precisely, consider the following:

I Given a polynomial $f \in \mathbb{Z}[v,x,y]$, decide the sentence $\exists v\ \forall x\ \exists y\ f(v,x,y) \stackrel{?}{=} 0$, with all three quantifiers ranging over $\mathbb{N}$ (or $\mathbb{Z}$).

II Given polynomials $f_1, \ldots, f_m \in \mathbb{Z}[x_1, \ldots, x_n]$ with $m \geq n$, decide if there is a **rational** solution to $f_1 = \cdots = f_m = 0$.

We show that problem (I) can be done within **coNP** for almost all inputs. The decidability of problem (I), over $\mathbb{N}$ and $\mathbb{Z}$, was previously unknown. We also show that the **Generalized Riemann Hypothesis (GRH)** implies that problem (II) can be solved within the complexity class $\mathbf{P}^{\mathbf{NP}^{\mathbf{NP}}}$ for almost all inputs, i.e., within the third level of the polynomial hierarchy. The decidability of problem (II), even in the case $m = n = 2$, remains open in general.

Along the way, we prove results relating polynomial system solving over $\mathbb{C}$, $\mathbb{Q}$, and $\mathbb{Z}/p\mathbb{Z}$. We also prove a result on Galois groups associated to sparse polynomial systems which may be of independent interest. A practical observation is that the aforementioned Diophantine problems should perhaps be avoided in the construction of crypto-systems.

## 1. INTRODUCTION AND MAIN RESULTS

The negative solution of Hilbert's Tenth Problem [Mat70, Mat93] has all but dashed earlier hopes of solving large polynomial systems over the integers. However,

[1] An extended abstract of this work appeared earlier in the Proceedings of the 31st Annual ACM Symposium on Theory of Computing (STOC, May 1–4, 1999, Atlanta, Georgia), 527–536, ACM Press, 1999. This research was supported by Hong Kong UGC Grant #9040469-730.

[2] URL: `http://math.cityu.edu.hk/~mamrojas`

[3] Department of Mathematics, City University of Hong Kong, 83 Tat Chee Avenue, Kowloon, HONG KONG (until December 2000).

an immediate positive consequence is the creation of a rich and diverse garden of hard problems with potential applications in complexity theory, cryptology, and logic. Even more compelling is the question of where the boundary to decidability lies.

From high school algebra we know that detecting and even finding roots in $\mathbb{Q}$ (or $\mathbb{Z}$ or $\mathbb{N}$) for polynomials in $\mathbb{Z}[x_1]$ is tractable. (We respectively use $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}$, and $\mathbb{N}$ for the complex numbers, real numbers, rational numbers, integers, and positive integers.) However, in [Jon82], James P. Jones showed that detecting roots in $\mathbb{N}^9$ for polynomials in $\mathbb{Z}[x_1, \ldots, x_9]$ is already undecidable.[4] Put another way, this means that determining the existence of a positive integral point on a general algebraic hypersurface of (complex) dimension 8 is undecidable.

It then comes as quite a shock that decades of number theory still haven't settled the complexity of the analogous question for algebraic sets of dimension 1 through 7. In fact, even the case of plane curves remains a mystery:[5] As of late 2000, the decidability of detecting a root in $\mathbb{N}^2$, $\mathbb{Z}^2$, or even $\mathbb{Q}^2$, for an **arbitrary** polynomial in $\mathbb{Z}[x_1, x_2]$, is still completely open.

### 1.1. Dimensions One and Two

To reconsider the complexity of detecting integral points on algebraic sets of dimension $\geq 1$, one can consider subtler combinations of quantifiers, and thus subtler questions on the disposition of integral roots, to facilitate finding decisive results. For example, Matiyasevich and Julia Robinson have shown [MR74, Jon81] that sentences of the form $\exists u\ \exists v\ \forall x\ \exists y\ f(u,v,x,y) \stackrel{?}{=} 0$ (quantified over $\mathbb{N}$), for **arbitrary** input $f \in \mathbb{Z}[u,v,x,y]$, are already undecidable. As another example of the richness of Diophantine sentences, Adleman and Manders have shown that deciding a very special case of the prefix $\exists\exists$ (quantified over $\mathbb{N}$) is **NP**-complete [AM75]: they show **NP**-completeness for the set of $(a,b,c) \in \mathbb{N}^3$ such that $ax^2 + by = c$ has a solution $(x,y) \in \mathbb{N}^2$.

However, the decidability of sentences of the form $\exists v\ \forall x\ \exists y\ f(v,x,y) \stackrel{?}{=} 0$ (quantified over $\mathbb{N}$ or $\mathbb{Z}$) was an open question — until recently: In [Roj00a] it was shown that (over $\mathbb{N}$) these sentences can be decided by a Turing machine, once the input $f$ is suitably restricted. Roughly speaking, deciding the prefix $\exists\forall\exists$ is equivalent to determining whether an algebraic surface has a slice (parallel to the $(x,y)$-plane) densely peppered with integral points. The "exceptional" $f$ not covered by the algorithm of [Roj00a] form a very slim subset of $\mathbb{Z}[v,x,y]$.

We will further improve this result by showing that, under similarly mild input restrictions, $\exists\forall\exists$ can in fact be decided within **coNP**. (This improves a **PSPACE** bound which appeared earlier in the proceedings version of this paper [Roj99a].) To make this more precise, let us write any $f \in \mathbb{Z}[v,x,y]$ as $f(v,x,y) = \sum c_a v^{a_1} x^{a_2} y^{a_3}$, where the sum is over certain $a := (a_1, a_2, a_3) \in \mathbb{Z}^3$. We then define the **Newton polytope of $f$**, **Newt($f$)**, as the convex hull of[6] $\{a \mid c_a \neq 0\}$. Also, when we say that

[4] This is currently one of the most refined statements of the undecidability of Hilbert's Tenth Problem.

[5] In particular, the major "solved" special cases so far have only extremely ineffective complexity and height bounds. (See, e.g., the introduction and references of [Roj00a].)

[6] i.e., smallest convex set in $\mathbb{R}^3$ containing...

a statement involving a set of parameters $\{c_1, \ldots, c_N\}$ is true **generically**[7], we will mean that for any $M \in \mathbb{N}$, the statement fails for at most $\mathcal{O}(N(2M+1)^{N-1})$ of the $(c_1, \ldots, c_N)$ lying in $\{-M, \ldots, M\}^N$. Finally, for an algorithm with a polynomial $f \in \mathbb{Z}[v, x, y]$ as input, speaking of the **dense encoding** will simply mean measuring the input size as $d + \sigma(f)$, where $d$ (resp. $\sigma(f)$) is the total degree[8] (resp. maximum bit-length of a coefficient) of $f$.

THEOREM 1.1. *Fix the Newton polytope $P$ of a polynomial $f \in \mathbb{Z}[v, x, y]$ and suppose that $P$ has at least one integral point in its interior. Assume further that we measure input size via the dense encoding. Then, for a generic choice of coefficients depending only on $P$, we can decide whether $\exists v\ \forall x\ \exists y\ f(v, x, y) = 0$ (with all three quantifiers ranging over $\mathbb{N}$ or $\mathbb{Z}$) within* **coNP**. *Furthermore, we can check whether an input $f$ has generic coefficients within* **NC**.

REMARK 1.1. *It is an open question whether membership in* **coNP** *for the problem above continues to hold relative to the* **sparse** *encoding. We will describe the latter encoding shortly. Recall also that* $\mathbf{NC} \subseteq \mathbf{P} \subseteq \mathbf{coNP}$*, and the properness of each inclusion is unknown [Pap95].* ■

The generic choice above is clarified further in section 3. It is interesting to note that the exceptional case to our algorithm for $\exists\forall\exists$ judiciously contains an extremely hard number-theoretic problem: determining the existence of a point in $\mathbb{N}^2$ on an algebraic plane curve. (That $\mathbb{Z}[v, y]$ lies in our exceptional locus is easily checked.) More to the point, James P. Jones has conjectured [Jon81] that the decidabilities of the prefixes $\exists\forall\exists$ and $\exists\exists$, quantified over $\mathbb{N}$, are equivalent. Thus, while we have not settled Jones' conjecture, we have at least now shown that the decidability of $\exists\forall\exists$ hinges on a sub-problem much closer to $\exists\exists$.

It would be of considerable interest to push these techniques further to prove a complexity-theoretic reduction from $\exists\forall\exists$ to $\exists\exists$, or from $\exists\forall\exists$ to $\forall\exists$. This is because these particular reductions would be a first step toward reducing $\exists\exists\forall\exists$ to $\exists\exists\exists$, and thus finally settling Hilbert's Tenth Problem in three variables. Evidence for such a reduction is provided by another result relating (a) the size of the **largest** positive integral point on an algebraic plane curve with (b) detecting whether an algebraic surface possesses **any** integral point: Roughly speaking, it was shown in [Roj00a] that the computability of the function alluded to in (a) implies that the undecidability of $\exists\exists\forall\exists$ occurs only in a family of inputs nearly equivalent to $\exists\exists\exists$.

As for algebraic sets of dimension zero, one can in fact construct **PSPACE** algorithms to find all **rational** points [Roj99a]. However, deciding the **existence** of rational points, even for algebraic sets of dimension zero, is not yet known to lie within the polynomial hierarchy. So let us now consider the latter problem.

### 1.2. Dimension Zero

[7] We can in fact assert a much stronger condition, but this one suffices for our present purposes.
[8] i.e., the maximum of the sum of the exponents in any monomial term.

We will show that deciding feasibility over $\mathbb{Q}$, for most polynomial systems, can be done within the polynomial hierarchy, assuming the **Generalized**[9] **Riemann Hypothesis (GRH)** — a famous conjecture from number theory. To clarify this statement, let us first fix some notation and illustrate some of the difficulties presented by rational roots of polynomial systems. We will then describe a quantitative result depending on GRH before stating our main results on rational roots.

NOTATION *Let* $\mathbf{F} := (f_1, \ldots, f_m)$ *be a system of polynomials in* $\mathbb{Z}[x_1, \ldots, x_n]$ *and let* $\boldsymbol{Z_F}$ *be the zero set of* $F$ *in* $\mathbb{C}^n$. *The* **size** *of an integer* $c$ *is* $\mathbf{size(}\boldsymbol{c}\mathbf{)} := 1 + \lceil \log_2(|c|+1) \rceil$. *Similarly, the* **(sparse) size**, $\mathbf{size(}\boldsymbol{F}\mathbf{)}$, *of the polynomial system* $F$ *is simply the sum of the sizes of all the coefficients* **and** *exponents in its monomial term expansion.* ■

To see why it is not entirely trivial to find the rational roots of a general $F$ in time polynomial in the sparse size of $F$, consider the following two phenomenae:

**Q1** The number of positive integral roots of $F$ can actually be exponential in $n$: A simple example is the system $(x_1^2 - 3x_1 + 2, \ldots, x_n^2 - 3x_n + 2)$, with sparse size $\mathcal{O}(n)$ and root set $\{1, 2\}^n$. Whether the number of rational roots of $F$ can still be exponential in the sparse size of $F$ for **fixed** $n$ (even $n = 2$!) is currently unknown. ■

**Q2** For any **fixed** $n > 1$, the integral roots of $F$ can have coordinates with bit-length exponential in size$(F)$, thus ruling out one possible source of **NP** certificates: For example, the system $(x_1 - 2, x_2 - x_1^d, \ldots, x_n - x_{n-1}^d)$ has sparse size $\mathcal{O}(n \log d)$ but has $(2, 2^d, \ldots, 2^{d^{n-1}})$ as a root. ■

So restricting to deciding the existence of rational roots, as opposed to explicitly finding them, may be necessary if one wants complexity sub-exponential in the sparse size. Indeed, sub-exponential bounds are already unknown for $m = n = 2$, and even decidability is unknown in the case $F := y^2 + ax^3 + bx + c$ with $a$, $b$, $c$ arbitrary rational numbers [Sil95, ch. 8], i.e., the case $(m, n) = (1, 2)$. So restricting to the case where $Z_F$ is zero-dimensional is also crucial.

On the other hand, when $n = 1$, it is a pleasant surprise that one can find **all** rational roots in time polynomial in size$(F)$ [Len99]. (Note that this is **not** an immediate consequence of the famous Lenstra-Lenstra-Lovász factoring algorithm — the family of examples $x^d + ax + b$ already obstructs a trivial application of the latter algorithm.) So in order to extend Lenstra's result to general zero-dimensional algebraic sets, let us consider an approach **other** than the known **PSPACE** methods of resultants and Gröbner bases: reduction modulo specially chosen primes.

First note that averaging over many primes (as opposed to employing a single sufficiently large prime) is essentially unavoidable if one wants to use information from reductions modulo primes to decide the existence of rational roots. For example, from basic quadratic residue theory [HW79], we know that the number of roots $x_1^2 + 1 \bmod p$ is **not** constant for sufficiently large prime $p$. Similarly, Galois-

[9] The **Riemann Hypothesis (RH)** is an 1859 conjecture equivalent to a sharp quantitative statement on the distribution of primes. GRH can be phrased as a generalization of this statement to prime ideals in an arbitrary number field, and further background on these RH's can be found in [LO77, BS96].

theoretic restrictions are also necessary before using information mod $p$ to decide feasibility over $\mathbb{Q}$.

EXAMPLE 1.1. *Take $m=n=1$ and $F=f_1=(x_1^2-2)(x_1^2-7)(x_1^2-14)$. Clearly, $F$ has no rational roots. However, it is easily checked via Legendre symbols [Apo90, ch. 9] that $F$ has a root mod $p$ for* **all** *primes $p$. In particular, note that the Galois group here does not act transitively: there is no automorphism of $\overline{\mathbb{Q}}$ which fixes $\mathbb{Q}$ and sends, say, $\sqrt{2}$ to $\sqrt{7}$.* ■

So let us then make the following definition.

DEFINITION 1.1. *Let $\boldsymbol{\sigma(F)}$ denote the maximum bit-length of any coefficient of the monomial term expansion of $F$. Recall that $\boldsymbol{\pi(x)}$ denotes the number of primes $\leq x$. Let $\boldsymbol{\pi_F(x)}$ be the variation on $\pi(x)$ where we instead count the number of primes $p \leq x$ such that the mod $p$ reduction of $F$ has a root in $\mathbb{Z}/p\mathbb{Z}$. Finally, let $\boldsymbol{N_F(x)}$ be the* **weighted** *variant of $\pi_F(x)$ where we instead count the* **total**[10] *number of distinct roots of the mod $p$ reductions of $F$, summed over all primes $p \leq x$.* ■

One can then reasonably guess that behavior of the quantities $\frac{\pi_F(x)}{\pi(x)}$ and/or $\frac{N_F(x)}{\pi(x)}$ for large $x$ will tell us something about the existence of rational roots for $F$. This is indeed the case, but as we will soon see, the convergence of the first quantity to its limit is unfortunately too slow to permit any obvious algorithm using sub-exponential work. The second quantity will be more important for us algorithmically, so let us give new sharpened estimates (depending on GRH) for both quantities.

DEFINITION 1.2. *Let $\mathbf{O}$ and $e_i$ respectively denote the origin and the $i^{\text{th}}$ standard basis vector of $\mathbb{R}^n$, and normalize $n$-dimensional volume so that the standard $n$-simplex (with vertices $\mathbf{O}, e_1, \ldots, e_n$) has $n$-volume 1. Also let $\#$ denote set cardinality and $V_F := \mathrm{Vol}_n(Q_F)$, where $Q_F$ is the convex hull of the union of $\{\mathbf{O}, e_1, \ldots, e_n\}$ and the set of all exponent vectors of $F$.* ■

THEOREM 1.2. *Let $K := \mathbb{Q}(x_i \mid (x_1, \ldots, x_n) \in Z_F,\ i \in \{1, \ldots, n\})$ and let $r_F$ be*[11] *the number of maximal ideals in the ring $\mathbb{Q}[x_1, \ldots, x_n]/\langle f_1, \ldots, f_n \rangle$. (In particular, $r_F \geq 1$ for $\#Z_F \geq 1$, and for $m=n=1$ the quantity $r_F$ is just the number of distinct irreducible factors of $f_1$ over $\mathbb{Q}[x_1]$.) Then the truth of GRH implies the following two statements for all $x > 33766$:*

1. *Suppose $\infty > \#Z_F \geq 2$ and $\mathrm{Gal}(K/\mathbb{Q})$ acts transitively on $Z_F$. Then*

$$\frac{\pi_F(x)}{\pi(x)} < \left(1 - \frac{1}{\#Z_F}\right)\left(1 + \frac{(\#Z_F! + 1)\log^2 x + \#Z_F!\mathcal{O}(\#Z_F\sigma(h_F))\log x}{\sqrt{x}}\right)$$

[10] If the number of roots in $\mathbb{Z}/p\mathbb{Z}$ of the mod $p$ reduction of $F$ exceeds $\delta$, then we add $\delta$ (not $\Omega(p)$) to our total, where $\delta$ is as defined in section 4.1.

[11] In [Roj99a], $r_F$ was incorrectly defined as the number of rational roots of $F$.

2. *Suppose* $\#Z_F \geq 1$ *and* $\dim Z_F < n$. *Then independent of* $\mathrm{Gal}(K/\mathbb{Q})$, *we have*

$$\frac{\pi_F(x)}{\pi(x)} > \frac{1}{\delta}(r_F - b(F,x)) \quad \text{and} \quad \left|\frac{N_F(x)}{\pi(x)} - r_F\right| < b(F,x).$$

*where* $0 \leq b(F,x) < \frac{4\delta \log^2 x + \mathcal{O}(\delta\sigma(\hat{h}_F)(1+n\delta^5/\sqrt{x}))\log x}{\sqrt{x}}$, $0 \leq \sigma(h_F) \leq \sigma(\hat{h}_F) \leq \mathcal{O}(M_F[\sigma(F)+n\log d+\log m])$, $d$ *is the maximum degree of any* $f_i$, $\delta \leq V_F$, *and* $M_F$ *is no larger than the maximum number of lattice points in any translate of* $(n+1)Q_F$. *Furthermore, when* $m \leq n$ *and* $\#Z_F < \infty$, *we can replace every occurrence of* $\delta$ *above with* $\#Z_F$. *Finally, explicit formulae for the asymptotic estimates above appear in remarks 4.16 and 4.17 of section 4.2.*

REMARK 1.2. *The polytope volume* $V_F$, *and even the lattice point count* $M_F$, *are more natural than one might think:* $V_F$ *is an upper bound on the number of irreducible components of* $Z_F$ *(cf. theorem 2.5 of the next section) and* $M_F = \mathcal{O}(e^n V_F)$ *[Roj00c, sec. 6.1.1, lem. 2 and rem. 6]. Furthermore, it is easy to show that* $V_F \leq d^n$. *In fact,* $d^n$ *frequently exceeds* $V_F$ *by a factor exponential in* $n$ *[Roj00b, Roj00c].* ■

REMARK 1.3. *It seems likely that the quantity* $\delta$ *from theorem 1.2 can be replaced by the* **affine geometric degree** *[KPS00] and the hypotheses* $m \leq n$ *and* $\#Z_F < \infty$ *dropped. (The affine geometric degree agrees with* $\#Z_F$ *when* $\#Z_F < \infty$ *and can be significantly less than* $V_F$ *when* $\#Z_F = \infty$.*) This improvement will be pursued in future work.* ■

The upper bound from assertion (1) appears to be new, and the first lower bound from assertion (2) significantly improves earlier bounds appearing in [Koi96, Bür00] which, when rewritten in the shape of our bounds, had leading coefficients of $\frac{1}{d^n}$ or worse. Also, the special case of the first bound from assertion (2) with $m \leq n$ and $F$ forming a reduced regular sequence was independently discovered by Morais (see [Mor97, thm. F, pg. 11] or [HMPS00, thm. 11, pg. 10]). In this special case, Morais' bound (which depends on the affine geometric degree) is asymptotically sharper than our bound when $\#Z_F = \infty$, and our bound is asymptotically sharper when $\#Z_F < \infty$. We also point out that the bounds from [Mor97, thm. F, pg. 11] or [HMPS00, thm. 11, pg. 10] are stated less explicitly than our formula in remark 4.16 of section 4.1, and our proof of theorem 1.2 provides a simpler alternative framework which avoids the commutative algebra machinery used in [Mor97, HMPS00].

Part (1) of theorem 1.2 thus presents the main difference between "modular" feasibility testing over $\mathbb{C}$ and $\mathbb{Q}$: it is known [Koi96, thm. 1] that the mod $p$ reduction of $F$ has a root in $\mathbb{Z}/p\mathbb{Z}$ for a density of primes $p$ which is either positive or zero, according as $F$ has a root in $\mathbb{C}$ or not. (See also [Roj00c, sec. 2, thm. 4] for the best current quantitative bound along these lines.) The corresponding gap between densities is large enough to permit a coarse but fast approximate counting algorithm for $\#\mathbf{P}$ to be used to tell the difference, thus eventually yielding an **AM** algorithm for feasibility over $\mathbb{C}$ recently discovered by Pascal Koiran [Koi96]. (We point out

that Koiran's algorithm also relies on the behavior of the function $N_F$, which seems to behave better asymptotically than $\pi_F$.) On the other hand, part (1) of theorem 1.2 tells us that the mod $p$ reduction of $F$ has a root in $\mathbb{Z}/p\mathbb{Z}$ for a density of primes $p$ which is either 1 or $\leq 1 - \frac{1}{\#Z_F}$ (provided $2 \leq \#Z_F < \infty$), and the lower density occurs if $F$ is infeasible over $\mathbb{Q}$ in a strong sense.

Via a $\mathbf{P}^{\mathbf{NP}^{\mathbf{NP}}}$ constant-factor approximate counting algorithm of Stockmeyer [Sto85], we can then derive the following result.

THEOREM 1.3. [12] *Following the notation and assumptions above, assume further that $F$ fails to have a rational root $\Longleftrightarrow$ [$Z_F = \emptyset$ or $\mathrm{Gal}(K/\mathbb{Q})$ acts transitively on $Z_F$]. Then the truth of GRH implies that deciding whether $Z_F \cap \mathbb{Q}^n$ is empty can be done within $\mathbf{P}^{\mathbf{NP}^{\mathbf{NP}}}$. Furthermore, we can check the emptiness and finiteness of $Z_F$ unconditionally (resp. assuming GRH) within* **PSPACE** *(resp.* **AM***).*

We thus obtain a new arithmetic analogue of Koiran's feasibility result over $\mathbb{C}$ [Koi96]. Indeed, just as we noted for feasibility over $\mathbb{Q}$, the best unconditional complexity bound for feasibility over $\mathbb{C}$ is **PSPACE** [Can88]. However, as we have seen, transferring conditional speed-ups from $\mathbb{C}$ to $\mathbb{Q}$ presents some unexpected subtleties.

REMARK 1.4. *The truth of GRH has many other consequences in complexity theory. For example, the truth of GRH implies a polynomial time algorithm for deciding whether an input integer is prime [Mil76], an* **AM** *algorithm for deciding whether $Z_F$ is empty [Koi96], and an* **AM** *algorithm for deciding whether $Z_F$ is finite [Koi97].* ■

REMARK 1.5. *Recall that* $\mathbf{NP} \cup \mathbf{BPP} \subseteq \mathbf{AM} \subseteq \mathbf{coRP}^{\mathbf{NP}} \subseteq \mathbf{coNP}^{\mathbf{NP}} \subseteq \mathbf{P}^{\mathbf{NP}^{\mathbf{NP}}} \subseteq \cdots \subseteq \mathbf{PH} \subseteq \mathbf{P}^{\#\mathbf{P}} \subseteq \mathbf{PSPACE} \subseteq \mathbf{EXPTIME}$*, and the properness of each inclusion is unknown [Zac86, BM88, BF91, Pap95].* ■

REMARK 1.6. *It is quite possible that even without access to an oracle in $\mathbf{NP}^{\mathbf{NP}}$, the brute-force search implied by the algorithm from theorem 9, at least for a small number of primes, may be more practical than the usual tools of resultants and Gröbner bases. This remains to be checked extensively.* ■

Let us close with some observations on the strength of our last two theorems: First note that our restrictions on the input $F$ are actually rather gentle: In particular, if one fixes the monomial term structure of $F$ and assumes $m \geq n$, then it follows easily from the theory of resultants [GKZ94, Stu98, Roj99b] that, for a generic choice of the coefficients, $F$ will have only finitely many roots in $\mathbb{C}^n$. Furthermore, our hypothesis involving $\mathrm{Gal}(K/\mathbb{Q})$ holds nearly as frequently.

[12] This theorem corrects an alleged complexity bound of **AM**, which had an erroneous proof in [Roj99a].

THEOREM 1.4. *Following the notation above, assume $m \geq n$ and fix the monomial term structure of $F$ so that $Z_F \neq 1$ for a generic choice of the coefficients. Then, if one restricts to $F$ with integer coefficients of absolute value $\leq c$, the fraction of such $F$ with $\#Z_F < \infty$ and $\mathrm{Gal}(K/\mathbb{Q})$ acting transitively on $Z_F$ is at least $1 - \mathcal{O}(\frac{\log c}{\sqrt{c}})$. Furthermore, we can check whether $\mathrm{Gal}(K/\mathbb{Q})$ acts transitively on $Z_F$ within* **EXPTIME** *or, if one assumes GRH, within* $\mathbf{P}^{\mathbf{NP}^{\mathbf{NP}}}$.

Thus, if $m \geq n$ and the monomial term structure of $F$ is such that $\#Z_F \neq 1$ generically, it immediately follows that at least $1 - \mathcal{O}(\frac{\log c}{\sqrt{c}})$ of the $F$ specified above have no rational roots. The case where the monomial term structure of $F$ is such that $\#Z_F = 1$ generically is evidently quite rare, and will be addressed in future work.

REMARK 1.7. *A stronger result in the case $m = n = 1$ (sans complexity bounds) was derived by P. X. Gallagher in [Gal73]. Our more general result above follows from a combination of our framework here, the Lenstra-Lenstra-Lovasz (LLL) algorithm [LLL82], and an effective version of Hilbert's Irreducibility Theorem of Stephen D. Cohen [Coh81].* ■

Theorems 1.2–1.4 may thus be of independent interest to number theorists, as well as complexity theorists. Aside from a geometric trick, the proofs of theorems 1.2–1.4 share a particular tool in common with the proof of theorem 1.1: All four proofs make use of some incarnation of effective univariate reduction.

Theorems 1.1–1.4 are respectively proved in sections 3–6. However, let us first review some algorithmic tools that we will borrow from computational algebraic geometry and computational number theory.

## 2. BACKGROUND TOOLS

We begin with the following elementary fact arising from congruences.

PROPOSITION 2.1. *If $z$ is any* **rational** *root of $\alpha_0 + \alpha_1 x_1 + \cdots + \alpha_d x_1^d \in \mathbb{Z}[x_1]$, then $z = \pm\frac{b}{c}$ for some divisor $b$ of $\alpha_0$ and some divisor $c$ of $\alpha_d$.* ■

We will also need the following classical fact regarding the factors of a multivariate polynomial.

LEMMA 2.1. *[Mig92, pgs. 159–161] Suppose $f \in \mathbb{Z}[t_1, \ldots, t_N]$ has degree $d_i$ with respect to $t_i$ for all $i$ and coefficients of absolute value $\leq c$. Then $g \in \mathbb{Z}[t_1, \ldots, t_N]$ divides $f \Longrightarrow$ the coefficient of $t_1^{j_1} \cdots t_N^{j_N}$ in $g$ has absolute value $\leq c \prod_i \left( \binom{d_i}{j_i} \sqrt{(d_i + 1)} \right)$, for any $(j_1, \ldots, j_N) \in [d_1] \times \cdots \times [d_N]$. In particular, for $N = 1$, $\sigma(g) \leq \sigma(f) + (d_1 + \alpha) \log 2$, where $\alpha := 2 - \frac{3}{4 \log 2} < 0.91798$.* ■

We point out that the last assertion does not appear in [Mig92], but instead follows easily from Stirling's Estimate [Rud76, pg. 200, ex. 20].

We will also need some sufficiently precise quantitative bounds on the zero-dimensional part of an algebraic set, e.g., good bounds on the number of points and their sizes. A recent bound of this type, polynomial in $V_F$, is the following:

THEOREM 2.5. *[Roj00c, thms. 5 and 6] Following the notation of section 1.2, there are univariate polynomials* $P_1, \ldots, P_n, h_F \in \mathbb{Z}[t]$ *with the following properties:*

1. *The number of irreducible components of* $Z_F$ *is bounded above by the degree of* $h_F$, $\deg h_F$. *Furthermore,* $\deg P_1, \ldots, \deg P_n \leq \deg h_F \leq V_F$, *and* $\deg h_F = \#Z_F$ *when* $m \leq n$ *and* $\#Z_F < \infty$.
2. $\#Z_F < \infty \Longrightarrow$ *the splitting field of* $h_F$ *is exactly the field* $K = \mathbb{Q}[x_i \mid (x_1, \ldots, x_n) \in \mathbb{C}^n$ *is a root of* $F]$.
3. *Let* $Z'_F$ *denote the zero-dimensional part of* $Z_F$. *Then* $P_i(x_i) = 0$ *for any* $(x_1, \ldots, x_n) \in Z'_F$ *and any* $i \in \{1, \ldots, n\}$.
4. $\sigma(P_1), \ldots, \sigma(P_n) \leq \sigma(h_F) = \mathcal{O}(M_F[\sigma(F) + n \log d + \log m])$. ■

REMARK 2.8. *Quoting [Roj00c, sec. 6.1.1 lem. 2 and sec. 6.1.3, rem. 9], we can actually give explicit upper bounds for* $\sigma(h_F)$. *Letting* $\mu$ *(resp.* $k$*) denote the maximal number of monomial terms in any* $f_i$ *(resp. total number of monomial terms in* $F$*, counting repetitions amongst distinct* $f_i$*), the bounds are as follows:*

$$\log \left\{ \frac{16\sqrt{2}}{e^3} \frac{\sqrt{n+1}}{nV_F} 4^{M_F} \left( n^{3/2} \lceil n \underline{V_F} (\underline{V_F} - 1)/4 \rceil \right)^{V_F} \left( \sqrt{\mu} (c + \lceil k M_F / 2 \rceil) \right)^{M_F - V_F} \right\}$$

*if* $m \leq n$, *or*

$$\log \left\{ \frac{16\sqrt{2}}{e^3} \frac{\sqrt{n+1}}{nV_F} 4^{M_F} \left( n^{3/2} \lceil nV_F(V_F - 1)/4 \rceil \right)^{V_F} \left( \sqrt{\mu} (m \lceil mV_F/2 \rceil c + \lceil k M_F / 2 \rceil) \right)^{M_F - V_F} \right\}$$

*for* $m > n \geq 1$, *where* $M_F \leq e^{1/8} \frac{e^n}{\sqrt{n+1}} V_F + \prod_{i=1}^n (p_i + 2) - \prod_{i=1}^n (p_i + 1)$, *and* $p_i$ *is the length of the projection of* $nQ_F$ *onto the* $x_i$*-axis. (Note that* $e^{1/8} < 1.3315$ *and* $\frac{16\sqrt{2}}{e^3} < 1.127$.*)*

*Furthermore, if* $m \leq n$ *and* $\#Z_F < \infty$, *then we can replace the underlined occurences of* $V_F$ *by* $\#Z_F$, *provided we then add an extra summand of* $(V_F + \alpha) \log 2$ *(with* $\alpha := 2 - \frac{3}{4 \log 2} < 0.91798$*) to our bound for* $\sigma(h_F)$. ■

REMARK 2.9. *The true definition of the quantity* $M_F$ *depends on a particular class of algorithms for constructing the* **toric resultant** *(see [Roj00c] for further details on* $M_F$ *and toric resultants). Thus,* $M_F$ *is typically much smaller than the worst-case bound given above.*

A preliminary version of the above result was announced in the proceedings version of this paper [Roj99a]. Earlier quantitative results of this type, usually with stronger hypotheses or less refined bounds, can be found starting with the work of Joos Heintz and his school from the late 80's onward. A good reference for these earlier results is [KP96] and more recent bounds similar to the one above can be found in [KPS00, prop. 2.11] and [Mai00, cor. 8.2.3]. There are also more general versions of theorem 2.5 applying even to quantifier elimination over algebraically

closed fields, but the bounds get looser and the level of generality is greater than we need. (These bounds appear in [Koi96] and are a corollary of results from [FGM90].)

An immediate corollary of our quantitative result above is the following upper bound on $\pi(x) - \pi_F(x)$, which may be of independent interest.

COROLLARY 2.1. *Following the notation of theorem 2.5, assume $F$ has a rational root. Then the number of primes $p$ for which the mod $p$ reduction of $F$ has* **no** *roots in $\mathbb{Z}/p\mathbb{Z}$ is no greater than $a_F^* := n + \sum_{i=1}^n \sigma(P_i) = \mathcal{O}(nM_F[\sigma(F) + n\log d + \log m])$.*

**Proof:** Consider the $i^{\underline{\text{th}}}$ coordinate, $x_i$, of any rational root of $F$. By theorem 2.5, and an application of proposition 2.1, the log of the denominator of $x_i$ (if $x_i$ is written in lowest terms) can be no larger than $\sigma(P_i)$. In particular, this denominator must have no more than $\sigma(P_i)+1$ prime factors, since the only prime power smaller than $e$ is 2. Since we are dealing with $n$ coordinates, we can simply sum our last bound over $i$ and conclude. ■

Let $\mathbf{Li}(\boldsymbol{x}) := \int_2^x \frac{\mathrm{d}t}{\log t}$. The following result from analytic number theory will be of fundamental importance in our quantitative discussions on prime densities.

THEOREM 2.6. *The truth of RH implies that, for all $x > 2$, $\pi(x)$ is within a factor of $1 + \frac{7}{\log x}$ of $x(\frac{1}{\log x} + \frac{1}{\log^2 x}) - \frac{2}{\log 2}$. Furthermore, independent of RH, for all $x > 2$, $\mathrm{Li}(x)$ is within a factor of $1 + \frac{6}{\log x}$ of $x(\frac{1}{\log x} + \frac{1}{\log^2 x}) - \frac{2}{\log 2}$.* ■

The proof can be sketched as follows: One first approximates $\mathrm{Li}(x)$ within a multiple of $1 + \frac{6}{\log x}$ by $x(\frac{1}{\log x} + \frac{1}{\log^2 x}) - \frac{2}{\log 2}$, using a trick from [Apo90, pg. 80]. Then, a (conditional) version of the effective Chebotarev Density Theorem, due to Oesterlé [Oes79, BS96], tells us that the truth of RH implies

$$|\pi(x) - \mathrm{Li}(x)| < \sqrt{x}\log x, \quad \text{for all} \quad x > 2.$$

So, dividing through by $x(\frac{1}{\log x} + \frac{1}{\log^2 x}) - \frac{2}{\log 2}$ and applying the triangle inequality, we obtain our theorem above.

The remaining facts we need are more specific to the particular main theorems to be proved, so these will be mentioned as the need arises.

REMARK 2.10. *Henceforth, we will use a stronger definition of genericity: A statement involving a set of parameters $\{c_1, \ldots, c_N\}$ holds* **generically** *iff the statement is true for all $(c_1, \ldots, c_N) \in \mathbb{C}^N$ outside of some* **a priori fixed** *algebraic hypersurface. That this version of genericity implies the simplified version mentioned earlier in our theorems is immediate from Schwartz' Lemma [Sch80].* ■

## 3. GENUS ZERO VARIETIES AND THE PROOF OF THEOREM 1.1

In what follows, we will make use of some basic algebraic geometry. A more precise description of the tools we use can be found in [Roj00a]. Also, we will always use **geometric** (as opposed to arithmetic) genus for algebraic varieties [Har77].

Let us begin by clarifying the genericity condition of theorem 1.1. Let $Z_f$ be the zero set of $f$. What we will initially require of $f$ (in addition to the assumptions on

its Newton polytope) is that $Z_f$ be irreducible, nonsingular, and non-ruled. Later, we will see that a weaker and more easily verified condition suffices.

REMARK 3.11. *Ruled surfaces include those surfaces which contain an infinite family of lines, for example: planes, cones, one-sheeted hyperboloids, and products of a line with a curve. More precisely, an algebraic surface* $S \subseteq \mathbb{P}^N_{\mathbb{C}}$ *is called* **ruled** *iff there is a projective curve* $C$*, and a morphism* $\varphi : S \longrightarrow C$*, such that every fiber of* $\varphi$ *is isomorphic to* $\mathbb{P}^1_{\mathbb{C}}$*. We then call a surface* $S' \subseteq \mathbb{C}^3$ *(the case which concerns us)* **ruled** *iff* $S'$ *is isomorphic to an open subset of some ruled surface in* $\mathbb{P}^N_{\mathbb{C}}$*.* ■

LEMMA 3.1. *Following the notation and hypotheses of theorem 1.1, write* $f(v,x,y) := \sum_{(a_1,a_2,a_3)\in A} c_a v^{a_1} x^{a_2} y^{a_3}$*, where* $A \cap \{x_i = 0\} \neq \emptyset$ *for all* $i$*. Then, for a generic choice of the coefficients* $(c_a)_{a\in A}$*,* $Z_f$ *is irreducible, nonsingular, and non-ruled. In particular, for a generic choice of the coefficients, the set* $\Sigma_f := \{v_0 \in \mathbb{C} \mid \{(x,y) \in \mathbb{C}^2 \mid f(v_0,x,y)=0\}$ is singular or reducible$\}$ *is finite.*

**Proof:** First note that our hypothesis on $A$ simply prevents the coordinate hyperplanes from being subsets of $Z_f$. That $Z_f$ is irreducible and nonsingular for a generic choice of coefficients then follows easily from the Jacobian criterion for singularity [Mum95]. (One can even write the conditions explicitly via $\mathcal{A}$-discriminants [GKZ94], but this need not concern us here.)

That $Z_f$ is also non-ruled generically follows easily from a result of Askold G. Khovanski relating integral points in Newton polyhedra and genera [Kho78]: His result, given the hypotheses above, implies that $Z_f$ has positive genus for a generic choice of the coefficients. (In fact, the only assumptions necessary for his result are the Newton polytope condition stated in theorem 1.1 and the nonsingularity of $Z_f$.) The classification of algebraic surfaces [Bea96] then tells us that $Z_f$ has positive genus $\Longrightarrow$ $Z_f$ is non-ruled.

As for the assertion on $\Sigma_f$, assume momentarily that $Z_f$ is irreducible, nonsingular, and non-ruled. Then by Sard's theorem [Hir94], $Z_f \cap \{v = v_0\}$ is irreducible and nonsingular for all but finitely many $v_0 \in \mathbb{C}$. Thus, $\Sigma_f$ is finite when $Z_f$ is irreducible, nonsingular, and non-ruled.

Since the intersection of any two open Zariski-dense sets is open and dense, we are done. ■

LEMMA 3.2. *Following the notation above, the set of* $v_0 \in \mathbb{Z}$ *such that* $\forall x\ \exists y\ f(v_0,x,y) = 0$ *is contained in* $\Sigma_f \cap \mathbb{Z}$*, whether both quantifiers range over* $\mathbb{N}$ *or* $\mathbb{Z}$*. Furthermore,* $\Sigma_f \cap \mathbb{N}$ *finite* $\Longrightarrow$ *the number of elements of* $\Sigma_f \cap \mathbb{Z}$*, and the size of each such element, is polynomial in the dense encoding.*

**Proof:** By Siegel's Theorem [Sil99], $\forall x\ \exists y\ f(v_0,x,y) = 0 \Longrightarrow Z_f \cap \{v = v_0\}$ contains a curve of genus zero (whether the quantification is over $\mathbb{N}$ or $\mathbb{Z}$).

Now note that for all nonzero $v_0 \in \mathbb{C}$, the Newton polytope of $f$ (as a polynomial in **two** variables) is a polygon containing an integral point in its interior. So, by Khovanski's Theorem [Kho78] once again, $Z_f \cap \{v = v_0\}$ irreducible and nonsingular $\Longrightarrow$ $Z_f \cap \{v = v_0\}$ is a curve of positive genus.

Putting together our last two observations, the first part of our lemma follows immediately.

To prove the final assertion, note that the Jacobian criterion for singularity [Mum95] implies that $\Sigma_f$ is simply the set of $v_0$ such that $(v_0, x, y)$ is a complex root of the system of equations $(f(v_0, x, y), \frac{\partial f(v_0,x,y)}{\partial x}, \frac{\partial f(v_0,x,y)}{\partial y})$ has a solution $(x, y) \in \mathbb{C}^2$. Thus, $\Sigma_f \cap \mathbb{N}$ finite $\Longrightarrow \Sigma_f$ is a finite set, and by theorem 2.5 we are done. ■

Thanks to the following result, we can solve the prefix $\forall\exists$ within **coNP**.

TUNG'S THEOREM *[Tun87] Deciding the quantifier prefix $\forall\exists$ (with all quantifiers ranging over $\mathbb{N}$ or $\mathbb{Z}$) is* **coNP***-complete relative to the dense encoding.* ■

The algorithms for $\forall\exists$ alluded in Tung's Theorem are based on some very elegant algebraic facts due to James P. Jones, Andrzej Schinzel, and Shih-Ping Tung. We illustrate one such fact for the case of $\forall\exists$ over $\mathbb{N}$.

THE JST THEOREM *[Jon81, Sch82, Tun87] Given any $f \in \mathbb{Z}[x, y]$, we have that $\forall x\ \exists y\ f(x, y) = 0$ iff all three of the following conditions hold:*

*1. The polynomial $f$ factors into the form $f_0(x, y) \prod_{i=1}^{k} (y - f_i(x))$ where $k \geq 1$, $f_0(x, y) \in \mathbb{Q}[x, y]$ has* **no** *zeroes in the ring $\mathbb{Q}[x]$, and for all $i$, $f_i \in \mathbb{Q}[x]$ and the leading coefficient of $f_i$ is positive.*

*2. $\forall x \in \{1, \ldots, x_0\}\ \exists y \in \mathbb{N}$ such that $f(x, y) = 0$, where $x_0 = \max\{s_1, \ldots, s_k\}$ and, for all $i$, $s_i$ is the sum of the squares of the coefficients of $f_i$.*

*3. Let $\alpha$ be the least positive integer such that $\alpha f_1, \ldots, \alpha f_k \in \mathbb{Z}[x]$ and set $g_i := \alpha f_i$ for all $i$. Then the* **union** *of the solutions of the following $k$ congruences*

$$\begin{aligned} g_1(x) &\equiv 0 \ \mathbf{mod}\ \alpha \\ &\vdots \\ g_k(x) &\equiv 0 \ \mathbf{mod}\ \alpha \end{aligned} \qquad \textit{is } \mathbf{all} \textit{ of } \mathbb{Z}/\alpha\mathbb{Z}. \ ■$$

The analogue of the JST Theorem over $\mathbb{Z}$ is essentially the same, save for the absence of condition (2), and the removal of the sign check in condition (1) [Tun87].

**Proof of Theorem 1.1:** Within this proof, we will always use the **dense** encoding. Also note that if we are quantifying over $\mathbb{N}$, then the roots of $f$ on the coordinate hyperplanes can be ignored and we can assume (multiplying by a suitable monomial) that the Newton polytope of $f$ intersects very coordinate hyperplane.

Assume $\Sigma_f \cap \mathbb{N}$ is finite. **This** will be our genericity hypothesis and by lemma 3.1, and our hypothesis on the Newton polytope of $f$, this condition indeed occurs generically. Furthermore, via [Can88, NR96], we can check whether $\Sigma_f$ is finite (and thus whether $\Sigma_f \cap \mathbb{N}$ or $\Sigma_f \cap \mathbb{Z}$ is finite) within the class **NC**. It is then clear from lemma 3.2 that checking $\exists\forall\exists$ can now be reduced to checking an instance of $\forall\exists$ for every $v_0 \in \Sigma_f \cap \mathbb{N}$ (or $v_0 \in \Sigma_f \cap \mathbb{Z}$).

Our goal will then be to simply use **NP** certificates for finitely many false $\forall\exists$ sentences, or the emptiness of $\Sigma_f \cap \mathbb{N}$ (or $\Sigma_f \cap \mathbb{Z}$), as a single certificate of the falsity

of $\exists\forall\exists$. The emptiness of $\Sigma_f \cap \mathbb{N}$ (or $\Sigma_f \cap \mathbb{Z}$) can also be checked within the class **NC** [Can88]. So by lemma 3.2, it suffices to assume $\Sigma_f \cap \mathbb{N}$ is nonempty and then check that the size of each resulting certificate is polynomial in the dense size of $f$.

Fixing $v_0 \in \Sigma_f \cap \mathbb{Z}$, first note that the dense size of $f(v_0, x, y)$ is clearly polynomial in the dense size of $f(v, x, y)$, thanks to another application of lemma 3.2. A certificate of $\forall x\ \exists y\ f(v_0, x, y) \neq 0$ (quantified over $\mathbb{N}$) can then be constructed via the JST Theorem as follows: First, factor $f$ within **NC** (via, say, [BCGW92]). If $f$ has no linear factor of the form $y - f_i(x)$, then we can correctly declare that the instance of $\forall x\ \exists y\ f(v_0, x, y) \neq 0$ is true. Otherwise, we attempt to give an $x' \in \{1, \ldots, x_0\}$ such that $f(x', y)$ has no positive integral root. Should such an $x'$ exist, lemma 2.1 tells us that its size will be polynomial in size($f$), so $x'$ is an **NP** certificate. Otherwise, we give a pair $(j, t)$ with $1 \leq j \leq k$ and $t \in \{0, \ldots, \alpha\}$ such that $g_j(t) \not\equiv 0$ **mod** $\alpha$. Exhibiting such a pair gives a negative solution of an instance of the **covering congruence** problem, which is known to lie in **NP** [Tun87].

So we have now proved our main theorem in the case of quantification over $\mathbb{N}$. The proof of the case where we quantify over $\mathbb{Z}$ is nearly identical, simply using the aforementioned analogue of the JST Theorem over $\mathbb{Z}$ instead. ■

REMARK 3.12. *Note that if $f \in \mathbb{Z}[v, y]$ then the zero set of $f$ is a ruled surface in $\mathbb{C}^3$. From another point of view, the hypothesis of theorem 1.1 is violated since this $P$ has empty interior. Deciding $\exists\forall\exists$ for this case then reduces to deciding $\exists\exists$, which we've already observed is very hard. Nevertheless, Alan Baker has conjectured that the latter problem is decidable [Jon81, sec. 5].* ■

REMARK 3.13. *The complexity of deciding whether a given surface is ruled is an open problem. (Although one can check a slightly weaker condition ($\#\Sigma_f < \infty$) within* **NC***, as noted in our last proof.) It is also interesting to note that finding explicit parametrizations of* **rational** *surfaces (a special class of ruled surfaces) appears to be decidable. Evidence is provided by an algorithm of Josef Schicho which, while still lacking a termination proof, seems to work well in practice [Sch98].* ■

## 4. PRIME DISTRIBUTION: PROVING THEOREM 1.2

The proofs of assertions (1) and (2) will implicitly rely on another quantitative result on the factorization polynomials, which easily follows from Hadamard's inequality [Mig92].

DEFINITION 4.3. *Given any polynomial $f(x_1) = \alpha_0 + \alpha_1 x_1 + \cdots + \alpha_D x_1^D$, we define:*

$$\boldsymbol{\Delta_f} := \frac{(-1)^{D(D-1)/2}}{\alpha_D} \text{ DET} \begin{bmatrix} \alpha_0 & \cdots & \alpha_D & 0 & \cdots & 0 & 0 \\ 0 & \alpha_0 & \cdots & \alpha_D & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & \alpha_0 & \cdots & \alpha_D & 0 \\ 0 & 0 & \cdots & 0 & \alpha_0 & \cdots & \alpha_D \\ \alpha_1 & \cdots & D\alpha_D & 0 & \cdots & 0 & 0 \\ 0 & \alpha_1 & \cdots & D\alpha_D & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & \alpha_1 & \cdots & D\alpha_D & 0 \\ 0 & 0 & \cdots & 0 & \alpha_1 & \cdots & D\alpha_D \end{bmatrix},$$

*...where the first $D-1$ (resp. last $D$) rows of the matrix correspond to the coefficients of $f$ (resp. the derivative of $f$). The quantity $\Delta_f$ is also known as the* **discriminant of f**, *and vanishes only for polynomials with repeated roots [GKZ94].* ■

LEMMA 4.1. *Suppose $g \in \mathbb{Z}[x_1]$ is square-free and $\delta := \deg g$. Then*

$$\log|\Delta_g| \leq (2\delta-1)\sigma(f) + \frac{2\delta-1}{2}\log(\delta+1) + \frac{\delta}{2}\log(\delta(2\delta+1)/6). \quad \blacksquare$$

The last and most intricate result we will need is the following refined effective version of the primitive element theorem.

THEOREM 4.7. *[Roj00c, thm. 7] Following the notation of theorem 2.5, one can pick $\hat{h}_F \in \mathbb{Z}[t]$ (satisfying all the properties of $h_F$ from theorem 2.5), so that there also exist $a_1, \ldots, a_n \in \mathbb{N}$ and $h_1, \ldots, h_n \in \mathbb{Z}[t]$ with the following properties:*

1. *The degrees of $h_1, \ldots, h_n$ are all bounded above by $\deg(\hat{h}_F) \leq V_F$.*
2. *For any root $(\zeta_1, \ldots, \zeta_n) \in Z'_F$ of $F$, there is a root $\theta$ of $\hat{h}_F$ such that $\frac{h_i(\theta)}{a_i} = \zeta_i$ for all $i$.*
3. *For all $i$, both $\log a_i$ and $\sigma(h_i)$ are bounded above by $\mathcal{O}(V_F^5 \sigma(\hat{h}_F))$ and $\sigma(\hat{h}_F) = \mathcal{O}(\sigma(h_F))$.* ■

REMARK 4.14. *Quoting [Roj00c, sec. 6.1.5, rem. 11], we can actually make the asymptotic bounds above completely explicit:*

$$\sigma(h_i) \leq (2\delta^2-2\delta+1)\sigma(r) + (2\delta^2+1)\sigma(\hat{h}_F) + \log[(\delta^2+1)^{\delta^2}(\delta+1)^{\delta+1}(\delta^2-\delta+1)]$$

*and*

$$\log a_i \leq \delta(\delta-1)\sigma(r) + (\delta^2+1)\sigma(\hat{h}_F) + \frac{1}{2}\log[(\delta^2+1)^{\delta^2}(\delta+1)^{\delta}],$$

*where $\sigma(r) \leq \frac{\delta^2-\delta+2}{2}\log(B_1^2+\delta(\delta-1)/2)$, $B_1 := \left(\frac{4\cdot 16^{\delta+1}}{e^{9/4}} \cdot \sqrt{(\delta+1)^5}\right)^{\delta-1} e^{2(\delta-1)\sigma(\hat{h}_F)}$, $\delta := \max \deg h_i \leq \deg \hat{h}_F \leq V_F$, $\sigma(\hat{h}_F) \leq \sigma(h_F) + \delta' \log(2n+1) + (V_F+\alpha)\log 2$, $\delta' \leq V_F$, $\sigma(h_F)$ is bounded above as in remark 2.8 of section 2, and $\alpha := 2 - \frac{3}{4\log 2} < 0.91798$. (So $\log a_i$ actually admits an upper bound about half as large as the bound for $\sigma(h_i)$.)*

*Furthermore, when $m \leq n$ and $\#Z_F < \infty$, we can replace every occurence of $\delta$ and $\delta'$ above by $\#Z_F$.* ■

REMARK 4.15. *Earlier quantitative results of this type, e.g., those applied in [Koi96], had looser and less explicit bounds which were polynomial in* $d^{n^{\mathcal{O}(1)}}$. ■

### 4.1. Proving Assertion (2) of Theorem 1.2

First let us recall the following refined version of an important result due to Weinberger.

THEOREM 4.8. *Following the notation of lemma 4.1, suppose* $g \in \mathbb{Z}[x_1]$ *has degree* $\delta$ *and* **no** *factors of multiplicity* $>1$. *Then the truth of GRH implies that*

$$\left|\frac{N_g(x)}{\pi(x)} - r_g\right| < \frac{2\sqrt{x}\log(|\Delta_g|x^\delta) + \delta\log|\Delta_g|}{\mathrm{Li}(x)}, \quad \text{for all} \quad x > 2. \ \blacksquare$$

The original version from [Wei84] had an unspecified constant in place of the 2. The version above follows immediately from Weinberger's original proof, simply using a stronger version of effective Chebotarev than he used, i.e., one replaces theorem 1.1 of [LO77] by a result of Oesterlé [Oes79] (see also theorem 8.8.22 of [BS96]).

The second (harder) bound of assertion (2) of Theorem 1.2 is then just a simple corollary of theorems 2.5 and 4.8. The first bound is an even simpler corollary of the second bound.

**Proof of Assertion (2):** By theorems 2.5 and 4.7, it immediately follows that $r_F = r_{\hat{h}_F}$. (Note that $\hat{h}_F$ is square-free by construction.) It also follows easily that the mod $p$ reduction of $F$ has a root in $\mathbb{Z}/p\mathbb{Z} \Longrightarrow$ the mod $p$ reduction of $\hat{h}_F$ has a root in $\mathbb{Z}/p\mathbb{Z}$. Furthermore, theorem 4.7 tells us that a sufficient condition for the converse assertion is that $p$ not divide any of the $a_i$ (the denominators in our rational univariate representation of $Z_F$). We thus obtain $0 \leq N_{\hat{h}_F}(x) - N_F(x) \leq \delta\sum_{i=1}^n(\log a_i + 1)$, for all $x > 0$, where $\delta := \deg \hat{h}_F$.

Assume henceforth that $x > 2$. We then have

$$\left|\frac{N_F(x)}{\pi(x)} - r_F\right| \leq \left|\frac{N_{\hat{h}_F}(x)}{\pi(x)} - r_{\hat{h}_F}\right| + \frac{\delta(\sum_{i=1}^n \log a_i + n)}{\pi(x)}.$$

Combining theorem 4.8 and Oesterlé's conditional bound on $|\pi(x) - \mathrm{Li}(x)|$, we thus obtain that the truth of GRH implies

$$\left|\frac{N_F(x)}{\pi(x)} - r_F\right| < \frac{2\sqrt{x}\log(|\Delta_{\hat{h}_F}|x^\delta) + \delta\log|\Delta_{\hat{h}_F}|}{\mathrm{Li}(x)} + \left(1 + \frac{\sqrt{x}\log x}{\mathrm{Li}(x)}\right)\frac{\delta(\sum_{i=1}^n \log a_i + n)}{\mathrm{Li}(x)}.$$

By theorem 2.6, and the fact that $\frac{(\log^3 x)(1+6/\log x)}{\sqrt{x}(\log x+1)-\frac{2}{\log 2}\log^2 x} < 1$ for all $x > 33766$, we then obtain

$$\left|\frac{N_F(x)}{\pi(x)} - r_F\right| < \frac{2\sqrt{x}\log(|\Delta_{\hat{h}_F}|x^\delta) + \delta\log|\Delta_{\hat{h}_F}| + 2\delta(\sum_{i=1}^n \log a_i + n)}{\mathrm{Li}(x)},$$

for all $x > 33766$. The second bound from assertion (2) then follows immediately from lemma 4.1, theorem 2.5, and the fact that $\frac{\mathrm{Li}(x)}{x/\log x} < (1 + 4/\log x)^2$ (applying theorem 2.6 one last time).

The first bound of assertion (2) follows immediately from the second bound via a simple application of the triangle inequality and the inequality $N_F(x) \leq \delta \pi_F(x)$. ■

REMARK 4.16. *Carrying out the last step in detail (and observing that* $(1 + 4/\log x)^2 < 2$ *for all* $x > 33766$*) it is clear that the asymptotic bound on* $b(F, x)$ *can be replaced by the following explicit quantity:*

$$\frac{4\delta \log^2 x + \left(4 \log |\Delta_{\hat{h}_F}| + \frac{2\delta\left(\log |\Delta_{\hat{h}_F}| + 2n + 2\sum_{i=1}^{n} \log a_i\right)}{\sqrt{x}}\right) \log x}{\sqrt{x}},$$

*where* $\log |\Delta_{\hat{h}_F}| \leq (2\delta - 1)\sigma(\hat{h}_F) + \frac{2\delta - 1}{2} \log(\delta + 1) + \frac{\delta}{2} \log(\delta(2\delta + 1)/6)$, $\delta := \deg \hat{h}_F \leq V_F$, *and* $\hat{h}_F$ *and* $\log a_i$ *are as in theorem 4.7 and remark 4.14 of section 4.*

*Furthermore, via [Roj00c, sec. 6.1], we can conclude that every occurence of* $\delta$ *can be replaced by* $\#Z_F$ *when* $m \leq n$ *and* $\#Z_F < \infty$. ■

### 4.2. Proving Assertion (1) of Theorem 1.2

Here we will need the following result dealing with the density of primes for which the mod $p$ reduction of $F$ has a root in $\mathbb{Z}/p\mathbb{Z}$. This theorem may be of independent interest to computational number theorists.

THEOREM 4.9. *Following the notation of theorem 1.2, assume* $\#Z_F < \infty$ *and let* $j_F$ *be the fraction of elements of* $\mathrm{Gal}(K/\mathbb{Q})$ *which fix at least one root of* $F$*. Then the truth of GRH implies that*

$$\left| \frac{\pi_F(x)}{\pi(x)} - j_F \right| < \frac{j_F(V_F! + 1) \log^2 x + 2\left(j_F V_F! \log |\Delta_g| + \frac{\sigma(h_F) + 1}{\sqrt{x}}\right) \log x}{\sqrt{x}},$$

*for all* $x > 33766$*, where* $h_F$ *is the polynomial from theorem 2.5 and* $g$ *is the square-free part of* $h_F$*.*

**Proof:** Let $g$ be the square-free part of the polynomial $h_F$ from theorem 2.5 and let $j_g$ be the fraction of elements of the Galois group of $g$ (over $\mathbb{Q}$) which fix at least one root of $g$, where $g$ is the square-free part of the polynomial $h_F$ from theorem 2.5. By essentially the same argument as the beginning of the proof of assertion (1), we obtain $j_F = j_g$. Similarly, we also obtain $0 \leq \pi_g(x) - \pi_F(x) \leq \sigma(h_F) + 1$ for all $x > 2$.

Note that $j_g$ is also the fraction of elements of the Galois group which give permutations (of the roots of $g$) possessing a fixed point. Oesterlé's (conditional) version of effective Chebotarev [Oes79, BS96] then tells us[13] that the truth of GRH

[13] His result is actually stated in terms of conjugacy classes, but since the number of fixed points of a Galois group element is stable under conjugacy, we can simply sum over conjugacy classes.

implies $|\pi_g(x) - j_g \mathrm{Li}(x)| \leq j_g\sqrt{x}(2\log|\Delta| + \mathfrak{d}\log x)$, where $\Delta$ is the discriminant of the splitting field of $g$ and $\mathfrak{d}$ is the degree of this field extension over $\mathbb{Q}$. Letting $\delta := \deg g$ (which is exactly $\#Z_F$ by construction), basic Galois theory tells us that $\mathfrak{d} \leq \#Z_F!$.

By Oesterlé's conditional bound on $|\pi(x) - \mathrm{Li}(x)|$ we then obtain

$$|\pi_g(x) - j_g\pi(x)| \leq j_g\sqrt{x}(2\log|\Delta| + (\mathfrak{d}+1)\log x).$$

Following essentially the same reasoning as the proof of assertion (2) we then obtain

$$\left|\frac{\pi_F(x)}{\pi(x)} - j_F\right| < \frac{j_g(\mathfrak{d}+1)\log^2 x + 2\left(j_g\log|\Delta| + \frac{\sigma(h_F)+1}{\sqrt{x}}\right)\log x}{\sqrt{x}},$$

for all $x > 33766$. Using the fact that $|\Delta| \leq |\Delta_g|^{\mathfrak{d}}$ [BS96, pg. 259], and applying lemma 4.1, we are done. ■

Of course, we must now estimate the quantity $j_F$. Fortunately, a good upper bound has already been derived by Peter J. Cameron and Arjeh M. Cohen, in answer to a 1991 question of Hendrik W. Lenstra.

THEOREM 4.10. *Suppose $G$ is any group acting transitively and faithfully on a set of $N$ elements and $j_G$ is the fraction of elements of $G$ with at least one fixed-point. Then $j_G \leq 1 - \frac{1}{N}$.* ■

The proof occupies the second page of [CC92] and requires only some basic group representation theory.[14] The upper bound is tight, but completely classifying the next lower values of $j_G$ currently requires the classification of finite simple groups [GW97]. The latter classification will **not** be necessary for our results.

**Proof of Assertion (1):** Following the notation of our last proof, recall that $g$ is the square-free part of the polynomial $h_F$ from theorem 2.5. Then by assumption, $V_F \geq \#Z_F \geq 2$ and $\delta = \#Z_F$. Furthermore, by theorems 2.5 and 4.10, $j_F \leq 1 - \frac{1}{\#Z_F}$. So by theorem 4.9 we are done. ■

REMARK 4.17. *From our proofs above we easily see that the asymptotic bound from assertion (1) can be replaced by the following explicit quantity:*

$$\left(1 - \frac{1}{\#Z_F}\right)\left(1 + \frac{(\#Z_F! + 1)\log^2 x + 2\left(\#Z_F!\log|\Delta_g| + \frac{\#Z_F}{\#Z_F - 1}\cdot\frac{\sigma(h_F)+1}{\sqrt{x}}\right)\log x}{\sqrt{x}}\right),$$

*where $g$ is as in our proof above, $\log|\Delta_g| \leq 2(\delta-1)(\sigma(h_F) + (V_F + \alpha)\log 2) + \frac{2\delta-1}{2}\log(\delta+1) + \frac{\delta}{2}\log(\delta(2\delta+1)/6)$ (thanks to lemmata 2.1 and 4.1), $\alpha := 2 - \frac{3}{4\log 2} < 0.91798$, and $\sigma(h_F)$ is bounded as in remark 2.8 of section 2.* ■

## 5. THE PROOF OF THEOREM 9

[14] Their paper actually dealt with finding a **lower** bound for the quantity $1 - j_G$.

Our algorithm essentially boils down to checking whether $r_F \geq 2$ or $r_F = 1$, following the notation of theorem 1.2. Via our initial assumptions on $F$, we will see that this is the same as checking whether $F$ as a rational root or not.

REMARK 5.18. *It is at this point that we must slightly alter our defintion of $N_F$: As we sum the number of roots in $\mathbb{Z}/p\mathbb{Z}$ of the mod $p$ reductions of $F$, we instead add $V_F$ to our total for each $p$ where this number of roots exceeds $V_F$. This ensures that $N_F$ can actually be computed within $\#\mathbf{P}$, since $V_F$ can be computed within $\#\mathbf{P}$ (see below). It is unknown whether the same is true for the quantity $\delta$ in our initial definition of $N_F$.* ■

Our algorithm proceeds as follows: First check whether $Z_F$ is empty. If so, then we immediately know that $Z_F \cap \mathbb{Q}^n$ is empty and we are done. Otherwise, approximate $N_F(M)$ and $\pi(M)$ within a factor of $\frac{9}{8}$, where $M$ is an integer sufficiently larger than 33766 so that $b(F, M) < \frac{1}{10}$. Respectively calling these approximations $\bar{N}$ and $\bar{\pi}$, we then do the following: If $\bar{N} \leq (\frac{9}{8})^2 \bar{\pi}$, declare $Z_F \cap \mathbb{Q}^n$ empty. Otherwise, declare $Z_F \cap \mathbb{Q}^n$ nonempty.

That our algorithm works is easily checked. First note that $\bar{N} \leq (\frac{9}{8})^2 \bar{\pi} \iff \frac{N_F(M)}{\pi(M)} \leq (\frac{9}{8})^4$. So by theorem 1.2, our assumption on $b(F, M)$ implies that the last inequality occurs iff $r_F = 1$. (Note that we need GRH at this point.) Via theorem 4.7, and our earlier proofs, we know that $r_F = r_{\hat{h}_F}$. So by [Jac85, thm. 4.14], we have that $\mathrm{Gal}(K/\mathbb{Q})$ acts transitively on $Z_F$ iff $\hat{h}_F$ is irreducible over $\mathbb{Q}$ (or equivalently, $r_F = r_{\hat{h}_F} = 1$). So by our initial assumptions on $F$, $r_F = 1$ iff $F$ has no rational roots. Thus, we now need only check the complexity of our algorithm.

That the emptiness and finiteness of $Z_F$ can be checked within **PSPACE** unconditionally goes back to [Can88]. That the truth of GRH implies both bounds can be lowered to **AM** is proved respectively in [Koi96] and [Koi97]. So now we need only check the complexity of computing $M$, $\bar{N}$, and $\bar{\pi}$.

It follows immediately from [Pra75] that $N_F(x)$ and $\pi(x)$ can be computed within $\#\mathbf{P}$. Also, via [GK94], $V_F$ can be computed within $\#\mathbf{P}$ as well. Furthermore, via theorems 1.2 and 2.5 (and the fact that $0 \leq \log V_F \leq n \log d$), the number of bits of $M$ is polynomial in the size of $F$. So by [Sto85], $M$, $\bar{N}$, and $\bar{\pi}$ can be computed within $\mathbf{P}^{\mathbf{NP}^{\mathbf{NP}}}$. Therefore, our algorithm runs within $\mathbf{P}^{\mathbf{NP}^{\mathbf{NP}}}$, assuming GRH. ■

REMARK 5.19. *It is an open problem whether theorem 9 continues to hold under the weaker condition that the* **real** *dimension of $Z_F$ is at most zero.* ■

## 6. THE PROOF OF THEOREM 1.4

If $m > n$ then it follows easily from Schwartz' Lemma [Sch80] that $F$ has **no** roots for at least a fraction of $1 - \mathcal{O}(\frac{1}{c})$ of our $F$. So we can assume $m = n$.

Consider now the toric resultant, $\mathcal{R}$, of $f_1, \ldots, f_n$ and $u_0 + u_1 x_1 + \cdots + u_n x_n$. (The classical resultant of Macaulay would suffice to prove a weaker version of our theorem here for a more limited family of monomial term structures.) Then, for indeterminate coefficients, $\mathcal{R}$ is a nonzero irreducible polynomial over $\mathbb{Z}$ adjoin $u_0, \ldots, u_n$ and the coefficients of $F$. More importantly, if the coefficients of $F$ are

**constants**, $\mathcal{R}$ is divisible by $u_0 - (\zeta_1 u_1 + \cdots + \zeta_n u_n)$, for any root $(\zeta_1, \ldots, \zeta_n) \in \mathbb{C}^n$ of $F$.

If it happens that $\mathcal{R}$ (in fully symbolic form) is the constant 1, then it follows from the degree formula for the toric resultant [GKZ94] that $Z_F$ is empty for a generic choice of the coefficients and there is nothing to prove. So let us assume $\mathcal{R}$ is not identically 1 in its full symbolic form.

By [Coh81] it then follows that a fraction of at most $\mathcal{O}(\frac{\log c}{\sqrt{c}})$ of the $F$ whose coefficients are **rational** numbers of (absolute multiplicative) height $\leq c$ result in $\mathcal{R}$ being a reducible polynomial over $\mathbb{Q}[u_0, \ldots, u_n]$. By rescaling, this easily implies that at most $\mathcal{O}(\frac{\log c}{\sqrt{c}})$ of the $F$ whose coefficients are **integers** of absolute value $\leq c$ result in $\mathcal{R}$ being reducible over $\mathbb{Q}[u_0, \ldots, u_n]$.

We now observe (say from [Roj00c, sec. 6]) that the polynomial $h_F$ from theorem 2.5 is nothing more than the resultant $\mathcal{R}$, for suitably chosen $u_1, \ldots, u_n$. (So in particular, $\mathcal{R}$ irreducible and nonzero $\Longrightarrow \#Z_F < \infty$.) So let us apply the Effective Hilbert Irreducibility Theorem from [Coh81] one more time to obtain such a choice of $u_1, \ldots, u_n$.

We then obtain that the fraction of our $F$ for which $\#Z_F < \infty$ and $h_F$ is irreducible over $\mathbb{Q}$ is at least $1 - \mathcal{O}(\frac{\log c}{\sqrt{c}})$. By [Jac85, thm. 4.14], $h_F$ is irreducible iff its Galois group acts transitively on its roots. So by theorem 2.5, our first assertion is proved.

That $\mathrm{Gal}(K/\mathbb{Q})$ acts transitively on $Z_F$ can be checked within $\mathbf{P}^{\mathbf{NP}^{\mathbf{NP}}}$ (assuming GRH) is already clear from the proof of theorem 9. To obtain the unconditional complexity bound, it clearly suffices to factor $h_F$ within **EXPTIME** and see whether $h_F$ is irreducible. Since theorem 2.5 tells us that the dense size of $h_F$ is exponential in size($F$), we can conclude via an application of the polynomial-time LLL factoring algorithm from [LLL82]. ■

## ACKNOWLEDGEMENTS

The author thanks Felipe Cucker, Jan Denef, Michael Fried, Teresa Krick, Jeff Lagarias, Luis-Miguel Pardo, and Bjorn Poonen for some very useful discussions, in person and via e-mail. In particular, Jan Denef pointed out the excellent reference [FJ86], and Michael Fried helped confirm a group-theoretic hope of the author (theorem 4.10). Special thanks go to Pascal Koiran for pointing out errors in earlier versions of theorems 1.2 and 9.

This paper is dedicated to Gretchen Davis, a remarkable educator who first inspired the author's interest in mathematics.

## REFERENCES

AM75. Adleman, Leonard and Manders, Kenneth, *"NP-Complete Decision Problems for Quadratic Polynomials,"* Eighth Annual ACM Symposium on Theory of Computing (Hershey, PA, 1976), pp. 23–29, Assoc. Comput. Mach., New York, 1976.

Apo90. Apostol, Tom M., *"Introduction to Analytic Number Theory,"* Undergraduate Texts in Mathematics, Springer-Verlag, New York-Heidelberg, 1976.

BF91. Babai, László and Fortnow, Lance, *"Arithmetization: a New Method in Structural Complexity Theory,"* Comput. Complexity **1** (1991), no. 1, 41–66.

BM88. Babai, László and Moran, Shlomo, *"Arthur-Merlin Games: A Randomized Proof System and a Hierarchy of Complexity Classes,"* Journal of Computer and System Sciences, 36:254–276, 1988.

BS96. Bach, Eric and Shallit, Jeff, *Algorithmic Number Theory, Vol. I: Efficient Algorithms,* MIT Press, Cambridge, MA, 1996.

BCGW92. Bajaj, Chanderjit; Canny, John F.; Garrity, Thomas; Warren, Joe, *"Factoring Rational Polynomials Over the Complex Numbers,"* SIAM J. Computing 22 (1993), no. 2, pp. 318–331.

Bea96. Beauville, Arnaud, *Complex Algebraic Surfaces,* second edition, London Mathematical Society Student Texts, 34, Cambridge University Press, 1996.

Bre76. Brent, Richard P., *"Fast Multiple-Precision Evaluation of Elementary Functions,"* J. Assoc. Comput. Mach. **23** (1976), no. 2, 242–251.

Bür00. Bürgisser, Peter, *"Cook's Versus Valiant's Hypothesis,"* Theoretical Computer Science, special issue in honor of Manuel Blum's $60^{\underline{\text{th}}}$ birthday, vol. 235, March, 2000.

CC92. Cameron, Peter J. and Cohen, Arjeh M., *"On the Number of Fixed Point Free Elements in a Permutation Group,"* A Collection of Contributions in Honour of Jack van Lint, Discrete Math. 106/107 (1992), 135–138.

Can88. Canny, John F., *"Some Algebraic and Geometric Computations in PSPACE,"* Proc. $20^{\underline{\text{th}}}$ ACM Symp. Theory of Computing, Chicago (1988), ACM Press.

Coh81. Cohen, Stephen D., *"The Distribution of Galois Groups and Hilbert's Irreducibility Theorem,"* Proc. London Math. Soc. (3) 43 (1981), no. 2, pp. 227–250.

FGM90. Fitchas, Noaï, Galligo, André, and Morgenstern, Jacques, *"Precise Sequential and Parallel Complexity Bounds for Quantifier Elimination Over Algebraically Closed Fields,"* Journal of Pure and Applied Algebra, 67:1–14, 1990.

FJ86. Fried, Michael D. and Jarden, Moshe, *Field Arithmetic,* Ergebnisse der Mathematik und ihrer Grenzgebiete (3), Springer-Verlag, Berlin-New York, 1986.

Gal73. Gallagher, P. X., *"The Large Sieve and Probabilistic Galois Theory,"* Analytic Number Theory (Proc. Sympos. Pure Math., Vol. XXIV, St. Louis, Mo., 1972), 91–101, Amer. Math. Soc., Providence, R.I., 1973.

Gal80. _____, *"Some Consequences of the Riemann Hypothesis,"* Acta. Arith. 37 (1980), pp. 339–343.

GKZ94. Gel'fand, Israel M.; Kapranov, Misha M.; and Zelevinsky, Andrei V., *Discriminants, Resultants and Multidimensional Determinants,* Birkhäuser, Boston, 1994.

GK94. Gritzmann, Peter and Klee, Victor, *"On the Complexity of Some Basic Problems in Computational Convexity II: Volume and Mixed Volumes,"* Polytopes: Abstract, Convex, and Computational (Scarborough, ON, 1993), pp. 373–466, NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci., 440, Kluwer Acad. Publ., Dordrecht, 1994.

GW97. Guralnick, Robert and Wang, Daqing, *"Bounds for Fixed Point Free Elements in a Transitive Group and Applications to Curves over Finite Fields,* Israel J. Math. 101 (1997), 255–287.

HMPS00. Hägele, Klemens; Morais, Juan Enrique; Pardo, Luis Miguel; Sombra, Martin, *"On the Intrinsic Complexity of the Arithmetic Nullstellensatz,"* Journal of Pure and Applied Algebra **146** (2000), no. 2, pp. 103–183.

HW79. Hardy, G. H. and Wright, E. M., *An Introduction to the Theory of Numbers,* Fifth Edition, The Clarendon Press, Oxford University Press, New York, 1979.

Har77. Hartshorne, Robin, *Algebraic Geometry,* Graduate Texts in Mathematics, No. 52, Springer-Verlag.

Hir94. Hirsch, Morris, *Differential Topology,* corrected reprint of the 1976 original, Graduate Texts in Mathematics, 33, Springer-Verlag, New York, 1994.

Jac85. Jacobson, Nathan, *Basic algebra I,* second edition, W. H. Freeman and Company, New York, 1985.

Jon81. Jones, James P., *"Classification of Quantifier Prefixes Over Diophantine Equations,"* Zeitschr. f. math. Logik und Grundlagen d. Math., Bd. 27, 403–410 (1981).

Jon82. _____, *"Universal Diophantine Equation,"* Journal of Symbolic Logic, 47 (3), 403–410 (1982).

Kho78. Khovanski, Askold G., *"Newton Polyhedra and the Genus of Complete Intersections,"* Functional Analysis (translated from Russian), Vol. 12, No. 1, January–March (1978), 51–61.

Knu98. Knuth, Donald, *The Art of Computer Programming II: Seminumerical Algorithms,* $3^{\underline{\text{rd}}}$ edition, Addison-Wesley, 1998.

Koi96. Koiran, Pascal, *"Hilbert's Nullstellensatz is in the Polynomial Hierarchy,"* DIMACS Technical Report 96-27, July 1996. (**Note:** This preprint considerably improves the published version which appeared in Journal of Complexity in 1996.)

Koi97. _____, *"Randomized and Deterministic Algorithms for the Dimension of Algebraic Varieties,"* Proceedings of the 38$^{\underline{\text{th}}}$ Annual IEEE Computer Society Conference on Foundations of Computer Science (FOCS), Oct. 20–22, 1997, ACM Press.

KP96. Krick, Teresa and Pardo, Luis-Miguel, *"A Computational Method for Diophantine Approximation,"* Algorithms in Algebraic Geometry and Applications (Santander, 1994), pp. 193–253, Progr. Math., 143, Birkhäuser, Basel, 1996.

KPS00. Krick, Teresa; Pardo, Luis-Miguel; and Sombra, Martin, *"Sharp Arithmetic Nullstellensatz,"* Duke Mathematical Journal, to appear, also downloadable from `http://xxx.lanl.gov/abs/math.AG/9911094`.

LO77. Lagarias, Jeff and Odlyzko, Andrew, *"Effective Versions of the Chebotarev Density Theorem,"* Algebraic Number Fields: $L$-functions and Galois Properties (Proc. Sympos. Univ. Durham, Durham, 1975), 409–464, Academic Press, London, 1977.

LLL82. Lenstra, Arjen K.; Lenstra, Hendrik W.; and Lovász, László, *"Factoring Polynomials with Rational Coefficients,"* Math. Ann. 261 (1982), no. 4, 515–534.

Len99. Lenstra, Hendrik W., *"Finding Small Degree Factors of Lacunary Polynomials,"* Number Theory in Progress, Vol. 1 (Zakopane-Kóscielisko, 1997), pp. 267–276, de Gruyter, Berlin, 1999.

Mai00. Maillot, Vincent, *"Géométrie D'Arakelov Des Variétés Toriques et Fibrés en Droites Intégrables,"* Mém. Soc. Math. France, to appear.

Mat70. Matiyasevich, Yuri V., *"The Diophantineness of Enumerable Sets,"* Soviet Math. Dokl. 11 (1970), 354–358.

Mat93. _____, *Hilbert's Tenth Problem,* MIT Press (1993).

MR74. Matiyasevich, Yuri V. and Robinson, Julia *"Two Universal 3-Quantifier Representations of Recursively Enumerable Sets,"* Teoriya Algorifmov i Matematicheskaya Logika (Volume dedicated to A. A. Markov), 112–123, Vychislitel'nyĭ Tsentr, Akademiya Nauk SSSR, Moscow (Russian).

Mig92. Mignotte, Maurice, *Mathematics for Computer Algebra,* translated from the French by Catherine Mignotte, Springer-Verlag, New York, 1992.

Mil76. Miller, Gary L., *"Riemann's Hypothesis and Tests for Primality,"* J. Comput. System Sci. **13** (1976), no. 3, 300–317.

Mor97. Morais, José Enrique, *"Resolucion Eficaz de Sistemas de Ecuaciones Polinomiales (Efficient Solution of Systems of Polynomial Equations),"* Ph.D. Thesis, Univ. Cantabria, Santander, 1997.

Mum95. Mumford, David, *Algebraic Geometry I: Complex Projective Varieties,* Reprint of the 1976 edition, Classics in Mathematics, Springer-Verlag, Berlin, 1995.

NR96. Neff, C. Andrew and Reif, John, *"An Efficient Algorithm for the Complex Roots Problem,"* Journal of Complexity **12** (1996), no. 2, 81–115.

Oes79. Oesterlé, Joseph, *"Versions Effectives du Théorème de Chebotarev sous l'Hypothèse de Riemann Généralisée,"* Astérisque **61** (1979), pp. 165–167.

Pap95. Papadimitriou, Christos H., *Computational Complexity,* Addison-Wesley, 1995.

Pra75. Pratt, Vaughan R., *"Every Prime has a Succinct Certificate,"* SIAM J. Comput. **4** (1975), 327–340.

Roj99a. Rojas, J. Maurice, *"On the Complexity of Diophantine Geometry in Low Dimensions,"* Proceedings of the 31$^{\underline{\text{st}}}$ Annual ACM Symposium on Theory of Computing (STOC '99, May 1-4, 1999, Atlanta, Georgia), 527-536, ACM Press, 1999.

Roj99b. _____, *"Solving Degenerate Sparse Polynomial Systems Faster,"* Journal of Symbolic Computation, vol. 28 (special issue on elimination theory), no. 1/2, July and August 1999, pp. 155–186.

Roj00a. _____, *"Uncomputably Large Integral Points on Algebraic Plane Curves?,"* Theoretical Computer Science, special issue in honor of Manuel Blum's 60$^{\underline{\text{th}}}$ birthday, vol. 235, March, 2000, pp. 145–162.

Roj00b. _____, *"Some Speed-Ups and Speed Limits for Real Algebraic Geometry,"* Journal of Complexity, FoCM 1999 special issue, vol. 16, no. 3 (sept. 2000), pp. 552–571.

Roj00c. _____, *"Algebraic Geometry Over Four Rings and the Frontier to Tractability,"* Contemporary Mathematics, Proceedings of a Conference on Hilbert's Tenth Problem and Related Subjects (University of Gent, November 1-5, 1999), edited by Jan Denef, Leonard Lipschitz, Thanases Pheidas, and Jan Van Geel, AMS Press, to appear.

Rud76. Rudin, Walter, *Principles of Mathematical Analysis,* 3rd edition, McGraw-Hill, 1976.

Sch98. Schicho, Josef, *"Rational Parametrization of Surfaces,"* Journal of Symbolic Computation **26** (1998), no. 1, 1–29.

Sch82. Schinzel, Andrzej, *Selected Topics on Polynomials,* Univ. of Michigan Press, Ann Arbor, 1982.

Sch80. Schwartz, Jacob T., *"Fast Probabilistic Algorithms for Verification of Polynomial Identities,"* J. of the ACM 27, 701–717, 1980.

Sil95. Silverman, Joseph H., *The Arithmetic of Elliptic Curves,* corrected reprint of the 1986 original, Graduate Texts in Mathematics 106, Springer-Verlag (1995).

Sil99. _____, *"On the Distribution of Integer Points on Curves of Genus Zero,"* Theoretical Computer Science, special issue in honor of Manuel Blum's 60th birthday, vol. 235, no. 1, March, 2000, pp. 163–170.

Sto85. Stockmeyer, Larry, *"On Approximation Algorithms for #**P**,"* SIAM Journal on Computing, 14(4):849–861, 1985.

Stu98. Sturmfels, Bernd, *"Introduction to Resultants,"* Applications of Computational Algebraic Geometry (San Diego, CA, 1997), 25–39, Proc. Sympos. Appl. Math., 53, Amer. Math. Soc., Providence, RI, 1998.

Tun87. Tung, Shih-Ping, *"Computational Complexities of Diophantine Equations with Parameters,"* Journal of Algorithms **8**, 324–336 (1987).

Wei84. Weinberger, Peter, *"Finding the Number of Factors of a Polynomial,"* Journal of Algorithms, 5:180–186, 1984.

Zac86. Zachos, S., *"Probabilistic Quantifiers, Adversaries, and Complexity Classes: An Overview,"* Proc. 1st Structure in Complexity Theory Conference, vol. 223, Lecture Notes in Computer Science, Springer-Verlag, 1986.